IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Embedded Visual Cryptography for Secret Color Images Sharing using Stamping Algorithm, Encryption and Decryption technique

Prof. N. N. Thorat[1], Snehal M. Kaware[1], Dhanashri D. Patil[1], Neha R. More[1]

Dept. of I.T., JSPM's Bhivarabai Sawant Institute of Technology &Research, Pune University, India.[1]

Abstract: Now-a-days, peoples are using emails for sharing their data. Sharing of secret information via emails is not that much secure as the information or data can be hacked easily by the third-party. In this current work we have proposed Visual Cryptographic Scheme for color images where the divided shares are enveloped in other images using stamping. The shares are generated using Random Number. Visual Cryptography Schemes (VCS) is a process of encrypting the image which hide the secret information present in images. In simple visual cryptographic technique encryption of secret image is done by splitting the image into n number of shares and the Stamping process is performed by overlapping k number of shares. It may helps to hide secret image. The decryption process of simple visual cryptographic system can be performed by a human eye so there is a possibility of security issues while using cryptography for sharing information. and to solve this problem we are using password technique. Previous methods faced some security issues like pixel expansion and noise troubleshoot the proposed system add more security to generated transparencies by applying an envelope to each shares by using stamping algorithm.

Keywords: Visual cryptography, shares, transparencies, stamping algorithm.

I. INTRODUCTION

Visual Cryptography is a type of encryption technique to conceal the information in images and decryption can be performed by the human eye if the proper key images are used. Visual cryptography was introduced by Naor and Shamir in the year 1994. In Visual Cryptography scheme the secret image is splitted into several random shares that look like noise. It is difficult to fetch the information from one of the share. Acceptable number of transparent shares is needed to disclose the information. The simplest way to implement this scheme is to stamp the two layers onto a transparent sheet. In Visual Cryptography Scheme (VCS) picture or text should be given as an input in the form of digital images to the system and the system forms 'n' (2<n) number of several images (called shares), which looks like images of random noise. The user has to load 'k' number of shares, where 2<k<n, from those 'n' number of shares to reveal the secret image. The main feature of this approach is that the secret image is decrypted easily by the human visual system without performing any complex calculation. Naor and Shamir's scheme can conceal the secret image in n distinct images called shares. The secret image can then be revealed by easily loading together as many as k of the shares. Each of the shares looks like a set of random pixels. Generally, any single share, before being loaded up with the others, discloses nothing about the secret image. Figures below describes an example for visual cryptography scheme suggested by Shyamalendu Kandar The most VCS produce the random noise like shares as output. The hackers are more interested in this type of random shares and these shares are difficult to recognize by the participants. To recover from these difficulties the proposed scheme uses meaningful shares. By using the stamping algorithm in Ref the shares are meaningful if the secret is binary. But in the case of color secret image the shares a partially meaningful due to high amount of random pixels. So in the proposed system a digital watermarking technique is used for stamping a cover image to the random share without any pixel expansion. The cover images are color images that are represented by 24 bits (8 bits in each plane). The random looking shares are represented by 8 bits. The proposed scheme digitally watermarks these 8 bits of a pixel into the 24 bit pixel of the cover image. This can be done by replacing the b Least Significant Bits (LSB) of each plane of the cover image. The proposed digital watermarking technique used for stamping is listed in Algorithm 2 .Password is combination of characters, digits, special symbols, uppercase letters, lowercase letters, and spaces. Password helps to keep the document secure as it provide an authentication to documents. The password would be free of repetition, dictionary words, usernames, pronouns, IDs, and any other predefined number or letter sequences.In our system the password is applied for each image. While decryption the receiver will get a password which will be require to reconstruct the original image.

II. EXISTING SYSTEM

1) Visual Cryptography for General Access Structure by Multi-pixel Encoding with Variable Block Size:

Authors: Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang

Multi-pixel encoding is a developing technique in visual cryptography which encodes more than single pixel for each run. In fact on the other hand its ability of encoding is poor. This paper put forth a novel multi-pixel encoding

which could encode several numbers of pixels for each run. The size of encoding at single run is parallel to the number of the continuous same pixels discovered during scanning of secret image. The proposed technique can work efficiently for chromatic images and general access structure without pixel expansion. The experimental results also show that it could accomplish high efficiency for encoding and better quality for overlapped images. [2]

2) Halftone Visual Cryptography:

Authors: Zhi Zhou, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo.

Visual cryptography conceals a secret binary image (SI) into shares of random binary order. If the shares are stamped onto transparencies, the secret image could be visually decrypted by overlapping a definite subset of transparencies. However, no secret information could be achieved from the overlapping of a closed subset. The binary structure of the shares, however, has no visual meaning and bottlenecks the objectives of visual cryptography. Extended visual cryptography was suggested recently to build up meaningful binary images as shares using hyper graph colourings, but the visual quality was very low. In this paper, a technique known as halftone visual cryptography is introduced to obtain visual cryptography via half toning. Depending on the blue-noise dithering principles, the designed method employs the cluster and void algorithm to encode a secret binary image into halftone shares (images) carrying considerable visual information. The simulation shows that the visual qualities of the generated halftone shares are better than any other available visual cryptography technique known to date. [3]

3) JOINT VISUAL CRYPTOGRAPHY AND WATERMARKING:

Authors: Ming Sun Fu. Oscar C. Au

This paper explains how to utilize watermarking technique for visual cryptography. Both visual cryptography and halftone watermarking comprises of a hidden secret image. But their concepts are different from each other. For visual cryptography, a set of share binary images is used to preserve the content of the hidden image. The hidden image can only be disclosed when sufficient share images are achieved. For watermarking, the hidden image is embedded in one halftone image while maintaining the quality of the watermarked halftone image. In this paper, Ming Sun Fu proposed a joint Visual-cryptography and watermarking (JVW) algorithm that has the advantages of both watermarking and visual cryptography. [4]

4) AN IMPROVED VISUAL CRYPTOGRAPHY SCHEME FOR SECRET HIDING:

Authors: R.Youmaran, A. Adler, A. Miri

Visual Cryptography is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.

III.PROPOSED METHODOLOGY

Visual Cryptography

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human visual system. The benefit of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into a number of parts let n. k-n secret sharing scheme is a special type of Visual Cryptographic technique where at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information while decryption the receiver will need a password to decrypt image.

Stamping Cover Images

The most VCS produce the random noise like shares as output. The hackers are more interested in this type of random shares and these shares are difficult to recognize by the participants. To recover from these difficulties the proposed scheme uses meaningful shares. By using the stamping algorithm in Ref the shares are meaningful if the secret is binary. But in the case of color secret image the shares a partially meaningful due to high amount of random pixels. So in the proposed system a digital watermarking technique is used for stamping a cover image to the random share without any pixel expansion.

The cover images are color images that are represented by 24 bits (8 bits in each plane). The random looking shares are represented by 8 bits. The proposed scheme digitally watermarks these 8 bits of a pixel into the 24 bit pixel of the cover image. This can be done by replacing the b Least Significant Bits (LSB) of each plane of the cover image. The proposed digital watermarking technique used for stamping is listed in Algorithm 2

Password

Password is combination of characters, digits, special symbols, uppercase letters, lowercase letters, and spaces. Password helps to keep the document secure as it provide an authentication to documents. The password would be free of repetition, dictionary words, usernames, pronouns, IDs, and any other predefined number or letter sequences.
In our system the password is applied for each image. While decryption the receiver will get a password which will be require to reconstruct the original image.

Overall Process

Step I: The source image is divided into n number of shares using k-n secret sharing visual cryptography scheme such that k number of shares is sufficient to reconstruct the encrypted image.

Step II: Each of the n shares generated in Step I is embedded into n number of different envelope images using LSB replacement.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

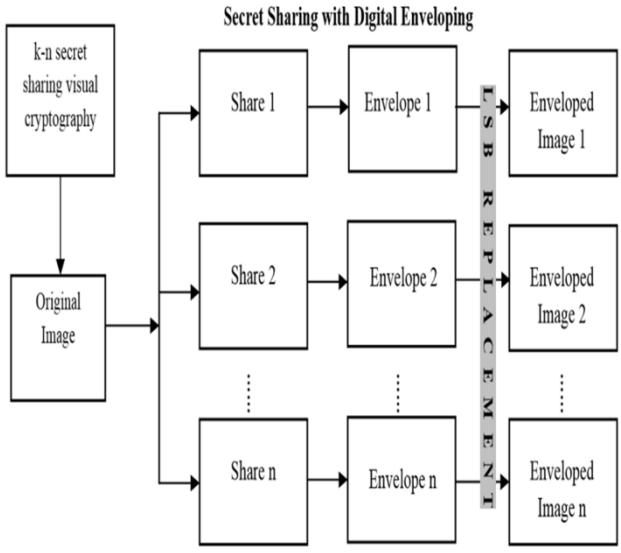
Step III: k number of enveloped images generated in Step II are taken and by using a password and LSB retrieving with OR operation, the original image is reconstruct.

System Architecture

1. **Encryption Process**

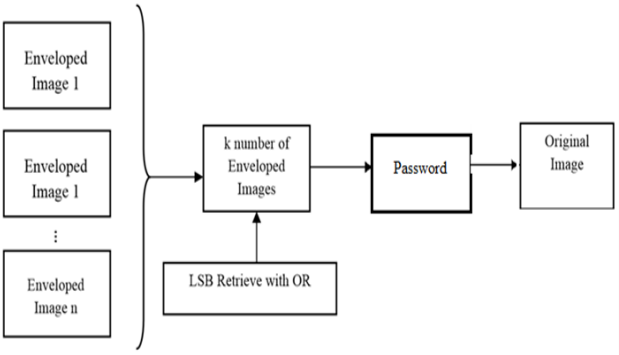
It consists of generation of shares using any basic visual cryptography model. In our proposed scheme, a (2, 2) VC share creation is performed. Each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub pixels. A black pixel is shared into two complementary blocks of four sub pixels. All the pixels in the secret image are encrypted similarly using this scheme. The shares can be either Vertical, Horizontal or Diagonal shares. Any single share is a random choice of two black and two white sub pixels, which looks medium grey. When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black).

The visual secret sharing scheme assumes that the message consists of a collection of colour pixels and each pixel is handled separately. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m sub pixels, which are printed in close proximity to each other so that the human visual system averages their individual contributions.



2. **Decryption Process**

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.In this step all n numbers of enveloped images are considered as input. Where each of these images for each pixel, the last two bits of alpha, red, green and blue (RGB) are retrieved and OR operation is performed to get the original image. The logic is that human visual system is acts as an OR function. For generated process the OR function can be used for the case of stacking n number of enveloped images.



Algorithm:-

1. k-n Secret Sharing Visual Cryptography Scheme:-

An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The division is done by the following algorithm.

Step I: Take an image IMG as input and calculate its width (w) and height (h).

Step II: Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image where k must be less than or equal to n. Calculate RECONS = (n-k)+1.

Step III: Create a three dimensional array IMG_SHARE[n][w*h][32] to store the pixels of n number of shares. k-n secret sharing visual cryptographic division is done by the following process.

```
for i = 0 to (w*h-1)
 {
   Scan each pixel value of IMG and convert it into 32 bit
binary string let PIX_ST.
for j = 0 to 31
  {
if (PIX_ST.charAt(i) =1){
call Random_Place (n, RECONS)
  }
for k = 0 to (RECONS−1)
    {
      Set IMG_SHARE [RAND[k]][i][j] = 1
    }
 }
```

Step IV: Create a one dimensional array IMG_CONS[n] to store constructed pixels of each n number of shares by the following process.

```
for k1 = 0 to (n-1)
{
for k2 = 0 to (w*h-1)
  {
    String value= “”
for k3 = 0 to 31 {
value = value+IMG_SHARE [k1][k2][k3]
  }
```

Construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0.

DOI 10.17148/IJARCCE.2016.5210

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Construct pixel from these part and store it into
IMG_CONS[k1] [4].
}
Generate image from IMG_CONS [k1]1 [8].
}
subroutine int Random_Place(n, RECONS)
{
Create an array RAND[RECONS] to store the generated random number.
for i = 0 to (recons-1)
{
Generate a random number within n, let rand_int. [9]
if(rand_int is not in RAND [RECONS])
RAND [i] = rand_int
}
return RAND [RECONS]
}

2. Encryption Algorithm

An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The encryption, i.e. division of the image into n number of shares such that k numbers of shares are sufficient to reconstruct the image; is done by the following algorithm.

Step: I: Take an image as input and calculate its width (w) and height (h).

Step II: Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image. k must be less than or equal to n.

Step III: Calculate recons=(n-k)+1.

Step IV: Create a three dimensional array img_share[n][w*h][32] to store the pixels of n number of shares.

3.k-n secret sharing of the original image using random sequence

Step I: The original image (Iw*h), number of shares to be divided (n) and number of shares needed (k) to retrieve the original image are taken as input

Step II: The number of sequences (ns) of (n−k+1) number of „1"s and (k −1) numbers of 0"s i.e. nCk−1 is calculated. Subsequently the sequences Sq1, Sq2, ….Sqns are constructed.

Step III: Let the shares of I denoted by S1, S2,…, Sn, each of size w X h. Shares are generated using the following logic.
i) Initialize all the bit positions of St by 0, for $1 \leq t \leq n$
ii) if (ith bit value of Ienc is 1)
{
Generate a random number „r" in the range 1 to ns.
Perform OR between the ith bit of Sj share
(where 1 j n) with the jth bit of the sequence Sqr ,
(1 r ns).
}

4. Proposed Stamping algorithm

Procedure Stamping (Shares, Covers)

1. Repeat for all shares
2. Repeat for each pixel of share

i) Generate an array S[0…8] that contain the bits of a pixel value

ii) Decompose the color cover into three components Red, Green, Blue and store bits of each component into three arrays R[0…8], G[0…8] and B[0…8] respectively.

iii) Find that which channel contain more information, i.e which color has less effect in the cover image.

iv) Replace the 2 least significant bits of the rest two channel with the share pixel value and 4 least significant bits of the channel that have less effect.

3. Stop

5. Decryption Process

In this step at least k numbers of enveloped images are taken as input. From each of these images for each pixel,the last two bits of alpha, red, green and blue are retrieved and OR operation is performed to generate the original image. It is already discussed that human visual system acts as an OR function. For computer generated process; OR function can be used for the case of stacking k number of enveloped images out of n. The ecryption process is performed by the following algorithm.

Step I: Input the number of enveloped images to be taken (k); height (h) and width (w) of each image.

Step II: Create a two dimensional array STORE[k][w*h*32] to store the pixel values of k number of enveloped images. Create a one dimensional array FINAL[(w/4)*h*32] to store the final pixel values of the image which will be produced by performing bitwise OR operation of the retrieved LSB of each enveloped images.

Step III:
for share_no = 0 to k-1
{
Take the name of the enveloped image to be taken and store the pixel values in STORE [share_no][w*h*32] using the following loop.
for i = 0 to (w*h-1)
{
Scan each pixel value of the Enveloped image and
Convert it into 32 bit binary string let PIX.
for j = 0 to 31
{
STORE[share_no][i*32+j] = PIX.charAt(j)
}
}
}

Step IV: Take a marker M= −1. Using the following process the last two bits of alpha, red, green and blue of each pixel of each k number of enveloped images are OR ed to produce the pixels of the original image.
for i = 0 to w*h
{
Consider 8 integer values from C0 to C7 and set all of them to 0.
for SH_NO = 0 to k-1

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

```
{
  c0 = c0 | STORE [SH_NO] [i*32+6]; // | is bitwise
  OR
   c1 = c1 | STORE [SH_NO] [i*32+7];
   c2 = c2 | STORE [SH_NO] [i*32+14];
   c3 = c3 | STORE [SH_NO] [i*32+15];
   c4 = c4 | STORE [SH_NO] [i*32+22];
    c5 = c5 | STORE [SH_NO] [i*32+23];
     c6 = c6 | STORE [SH_NO] [i*32+30];
    c7 = c7 | STORE [SH_NO] [i*32+31];
  }
        FINAL [++M] =c0;
        FINAL [++M] = c1;
        FINAL [++M] = c2;
        FINAL [++M] = c3;
        FINAL [++M] = c4;
        FINAL [++M] = c5;
        FINAL [++M] = c6;
        FINAL [++M] = c7;
}
```

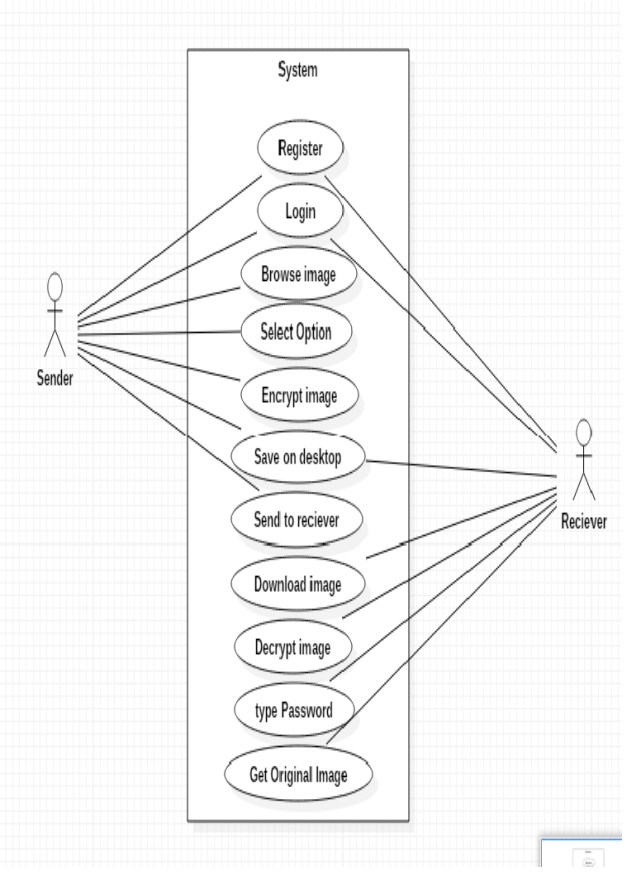
Create a one dimensional array IMG_CONS[ ] of size (w/4)*h to store constructed pixels.Construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring from FINAL[ ] starting from 0.

Construct pixel from these part and store it into

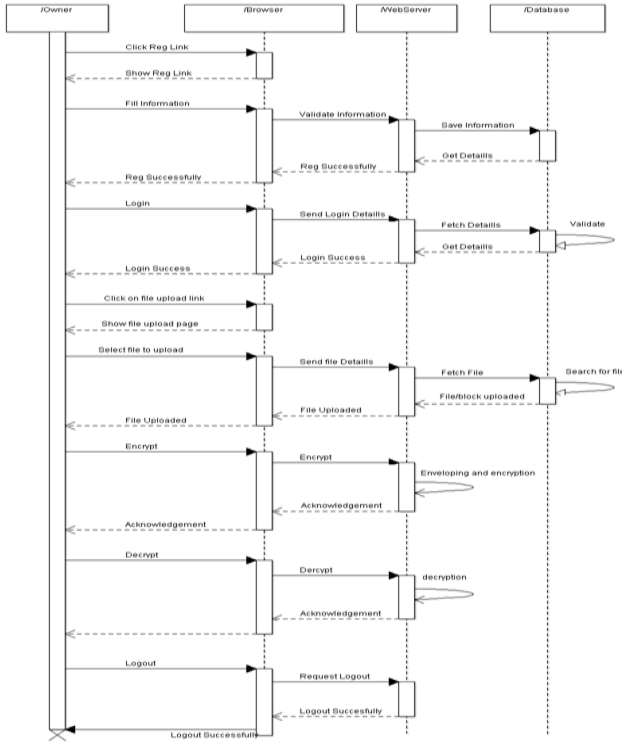
IMG_CONS[(w/4)*h]
Generate image from IMG_CONS[ ].

Design

Use case diagram



Sequence diagram



IV.CONCLUSION AND FUTURE WORK

Decryption process of simple visual cryptography is based on human vision system, so if a person gets competent k number of shares; the image can be easily decrypted. In this current work, with well-known k-n secret sharing visual cryptography technique an enveloping method is introduced where the secret shares are enveloped within clearly innocent covers of digital images using LSB replacement. This gives protection to visual cryptography scheme from unlawful attack as it fools the hackers' eye. The splitting of an image into n number of shares is done by using random number generator. This technique needs very few mathematical calculation compare to other available method s of visual cryptography on color images. This technique only checks '1' at the bit position and divide that '1' into (n-k+1) shares using random numbers. A comparison is made with the proposed scheme with some other schemes to prove the novelty of the scheme

Future Scope:-The future work involves the more number of shares and to implement the secret color video and share the multiple secret video by using various methods and also use OTP.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt'94, 1995, pp. 1–12.
[2] P. Ranjan, "Principles of Multimedia", Tata McGraw Hill,2006.
[3] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.
[4] Kandar Shyamalendu, Maiti Arnab, "K-N Secret Sharing Visual Cryptography Scheme For Color Image Using Random Number" International Journal of Engineering Science and Technology, Vol 3, No. 3, 2011, pp. 1851-1857.

[5] Naskar P., Chaudhuri A, Chaudhuri Atal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University, 2010, pp 62-65.
[6] Nakajima M, Yamaguchi Y, Extended Visual Cryptography for Natural Images, 10-th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision'2002
[7] Kumari K, Bhatia S, Multi-pixel Visual Cryptography for color images with Meaningful Shares, International Journal of Engineering Science and Technology Vol. 2(6), 2010
[8] Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking
[9] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

BIBLOGRAPHY

[1] Visual Cryptography and Its Applications
[2] Visual Cryptography and Secret Image Sharing. Stelvio Cimato, Ching-Nung Yang
[3] Visual Cryptography for Image Processing and Security Theory, Methods, and Applications
[4] Visual Cryptography and Its Applications by Jonathan Weir, WeiQi Yan

DOI 10.17148/IJARCCE.2016.5210